Shelter

管理者ツール

取扱説明書

第２版

ed-contrive®
イーディーコントライブ株式会社

目次

はじめに

Shelter 管理者ツールでできること----4
同梱品----4
動作環境----5
Shelter 管理者ツールのインストール----5

Shelter 管理者ツールの操作

Shelter 管理者ツールの起動----6
パスワード桁数の設定----6
パスワード使用文字種の設定----7
パスワードの必須使用文字種の設定----7
パスワードの有効期間の設定----8
24 時間内のパスワード変更可能回数の設定----8
パスワード履歴によるパスワード制限の設定----9
パスワード認証失敗制限回数の設定----9
ユーザードライブ遠隔ロック解除の設定----10
パスワードリマインダ機能の設定----10
マスターパスワードの設定----11
ドライブサイズの設定----11
ボリュームラベルの設定----12
追加ファイルの設定----12
アクセス許可プロセス（オフィス外用）の設定－①----13
アクセス許可プロセス（オフィス外用）の設定－②----14
流出防止オプション（オフィス外用）の設定----14
ログ取得機能の設定----15
ログファイル自動削除の設定----16
ウィンドウログの設定----17
プロセスログの設定----18
ファイルアクセスログの設定－①----19
ファイルアクセスログの設定－②----20
キーボードログの設定----21
インターネットアドレスログの設定----22
初期化ツール ID の設定----23
初期化ツール／オフィス内ドライバインストーラーの保存----23
設定内容の確認／設定の保存----24

ユーザードライブ遠隔ロック解除----------25

パスワードリマインダ----------26

初期化ツールの利用----------27

ソフトウェア環境毎の主な機能の比較----------28

ソフトウェア使用許諾書----------29

◎Microsoft、Windows、Windows 2000/XP/Vista は、Microsoft Corporation の米国及びその他の国における登録商標または商標です。
◎その他、記載されている会社名、製品名は各社の登録商標または商標です。

はじめに

Shelter 管理者ツールでできること

Shelter 管理者ツールは、セキュリティ USB メモリ「SD-Shelter」に対して、パスワードの桁数／使用可能文字種・ユーザードライブ遠隔ロック解除機能・パスワードリマインダ機能・ログ取得機能・オフィス外 PC でのネットワークアクセス／印刷の禁止 等、セキュリティポリシーの変更や機能追加を行なえるシステム管理者用ソフトウェアです。

Shelter 管理者ツールは、「初期化ツール」及び「Shelter オフィス内ドライバ」のインストーラーを作成するソフトウェアです。Shelter 管理者ツールで作成した初期化ツールをコピーして複数 PC で SD-Shelter の一斉書き換えや、初期化ツールだけを各拠点に配布等することにより、お客様自身が自由に個別設定を行うことができます。初期化する際には、「Shelter オフィス外ドライバ」のインストーラーとインストールマニュアル及び Shelter 機能の停止からアンマウントまでを行う「SDSStop」を SD-Shelter 内に作成します。

また、一度個別カスタマイズが行われた SD-Shelter では、予め設定した初期化ツール ID が一致しない限り、別の初期化ツール ID を持つ初期化ツールでの再設定ができませんので無断で設定が変更される心配がありません。

B 社/ 初期化ツール　　A 社用

同梱品

Shelter 管理者ツールには、次のものが同梱されています。開封後、ご確認ください。

① CD-ROM　1 枚

* 同梱品が足りないときや破損しているときは、当社もしくは販売店にご連絡ください。

動作環境

Shelter 管理者ツール

OS	Microsoft Windows 2000 Professional SP4 日本語版 Microsoft Windows XP Professional SP2/Home Edition SP2 日本語版 Microsoft Windows Vista 日本語版 * 64 ビット OS には、未対応
CPU	Intel Pentium III 1GHz 以上
メモリ	256MB 以上　* Vista に関しては 512MB 以上
その他	・管理者権限を持つアカウントでインストールする必要があります。 ・CD-ROM を再生できる倍速以上のドライブが必要です。

生成される初期化ツール

OS	Microsoft Windows 2000 Professional SP4 日本語版 Microsoft Windows XP Professional SP2/Home Edition SP2 日本語版 Microsoft Windows Vista 日本語版 * 64 ビット OS には、未対応
CPU	Intel Pentium III 1GHz 以上
メモリ	256MB 以上　* Vista に関しては 512MB 以上
対象 USB メモリ	SD-Shelter * 上記以外は対象外となります。
その他	・USB ポート　USB2.0 が必要です。 ・管理者権限を持つアカウントで実行する必要があります。

Shelter 管理者ツールのインストール

コンピュータの CD-ROM ドライブに Shelter 管理者ツールの CD を挿入します。CD-ROM ドライブの［Setup_SDSAdmin.exe］をダブルクリックします。インストーラーに従って操作してください。

＜Shelter 管理者ツールをアンインストールするには＞

［スタート］→［コントロールパネル］→［プログラムのアンインストール］（Windows XP の場合は［プログラムの追加と削除］、Windows 2000 の場合は［アプリケーションの追加と削除］）をクリックします。［SD-Shelter 管理者ツール］を選択し、アンインストールを行ってください。

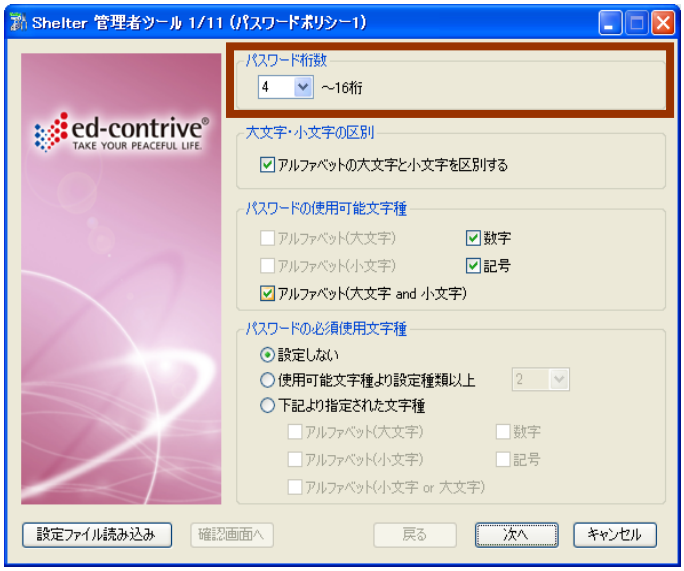
Shelter 管理者ツールの操作

Shelter 管理者ツールの起動

［スタート］→［(すべての) プログラム］→［ED-CONTRIVE］→［Shelter］→［Shelter 管理者ツール］を選択します。Shelter 管理者ツールが起動します。

パスワード桁数の設定

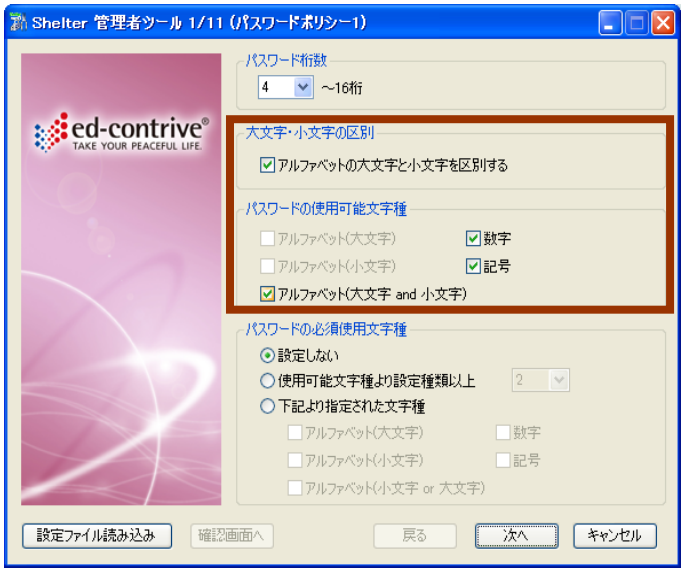
パスワードの最小桁数を 1～16 桁の間で設定可能です。(デフォルトは 4 桁です。)



パスワード使用文字種の設定

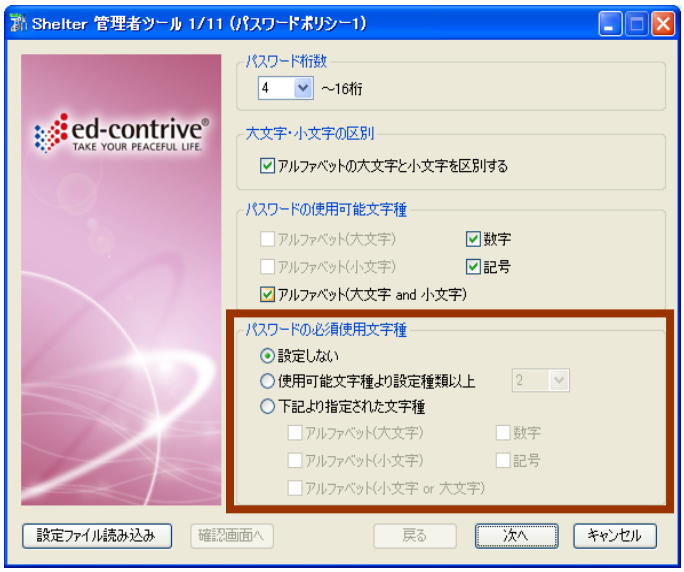
パスワードに使用する文字種が設定可能です。使用したい文字種を選択してください。（パスワードに使用する文字種は全て半角になります。）

アルファベットの大文字・小文字を区別しない場合は、入力された文字は全て大文字に変換して処理されます。



パスワードの必須使用文字種の設定

パスワードの入力必須文字種として設定したい文字種を選択してください。



パスワードポリシー1 の設定が完了したら、［次へ］をクリックします。

パスワードの有効期間の設定

パスワードの有効期間を設定する場合は［パスワードの有効期間日数を設定する］をチェックし、10 日～180 日の範囲で選択してください。

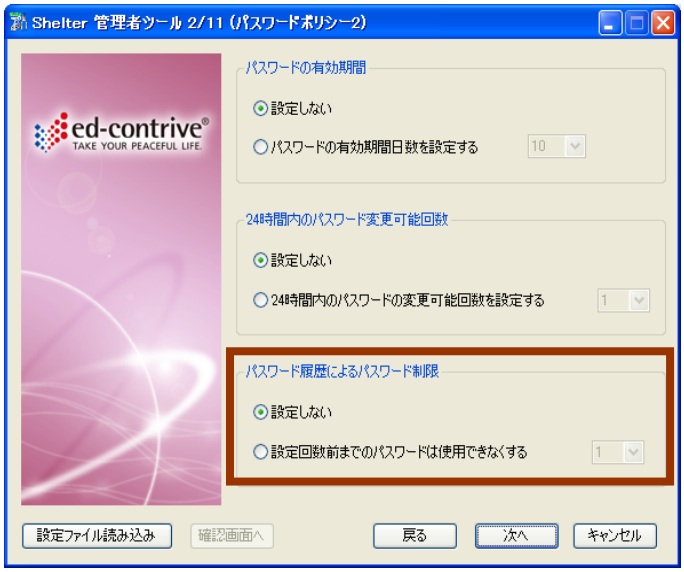
尚、パスワード設定時からパソコンの時間を戻す操作(24 時間以上)を実施した場合は、PC 時刻が正常でない可能性があると判断し、SD-Shelter 使用時にパスワード変更ダイアログが表示されます。

24 時間内のパスワード変更可能回数の設定

パスワードを 24 時間の間に変更可能な回数を設定します。初期パスワードの設定も 1 回としてカウントされます。

パスワード履歴によるパスワード制限の設定

過去に使用したことのあるパスワードを設定できないようにします。(現在使用しているパスワードを 1 回目としてカウントします)
履歴として 1～10 回目までのパスワードの禁止設定が可能です。

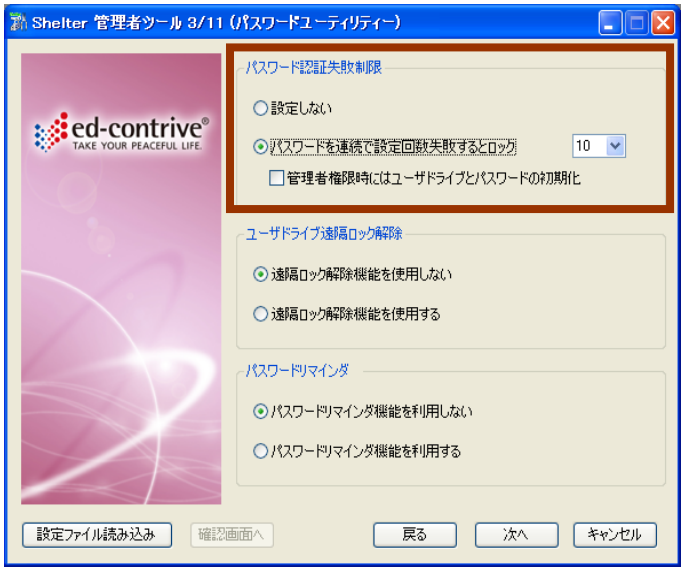


パスワードポリシー2 の設定が完了したら、［次へ］をクリックします。

パスワード認証失敗制限回数の設定

パスワード認証連続失敗回数の設定が可能です。設定した回数を超えてパスワード認証に失敗した場合は、SD-Shelter のユーザードライブはロックされ、正しいパスワードを入力しても使用できない状態となります。

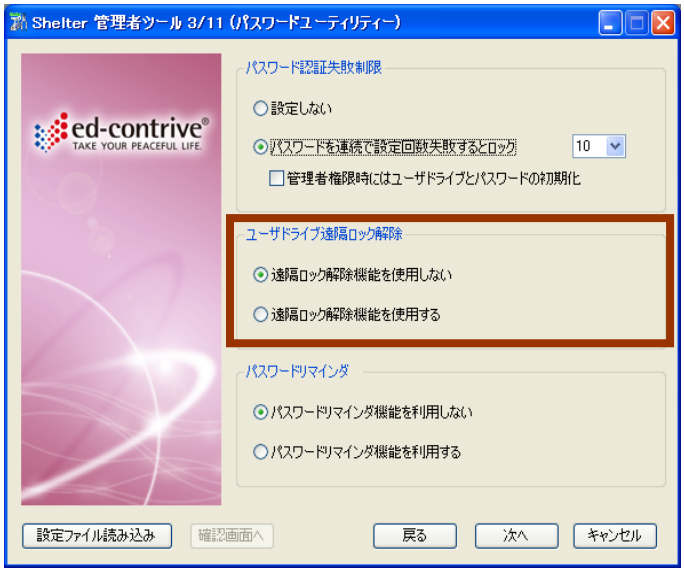
［管理者権限時にはユーザードライブとパスワードの初期化］をチェックすると、管理者権限でご利用の際に設定回数を超えるとロックではなく、パスワードとユーザードライブのデータを初期化します。



注意	* ［管理者権限時にはユーザードライブとパスワードの初期化］の実行後、パスワードポリシー等は引き継がれますが、ユーザードライブの追加ファイルやログファイルについては、復旧致しません。

ユーザードライブ遠隔ロック解除の設定

パスワード認証失敗制限回数の設定回数を超えてロックされた SD-Shelter をロック解除する機能です。
本機能を有効にすれば、SD-Shelter ロック時に、ロック解除用のコードを取得することができます。
ロック解除の操作については P.25 をご参照ください。

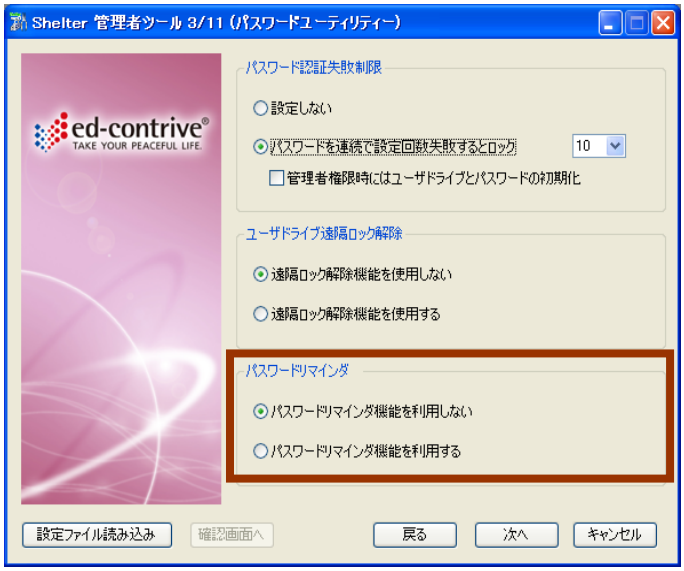


パスワードリマインダ機能の設定

パスワードリマインダ機能を有効にすると、SD-Shelter でリマインドコードを取得できます。

管理者は取得したリマインドコードを使用して設定しているパスワードを確認することが可能です。

パスワードリマインダの操作については P.26 をご参照ください。



パスワードユーティリティーの設定が完了したら、［次へ］をクリックします。

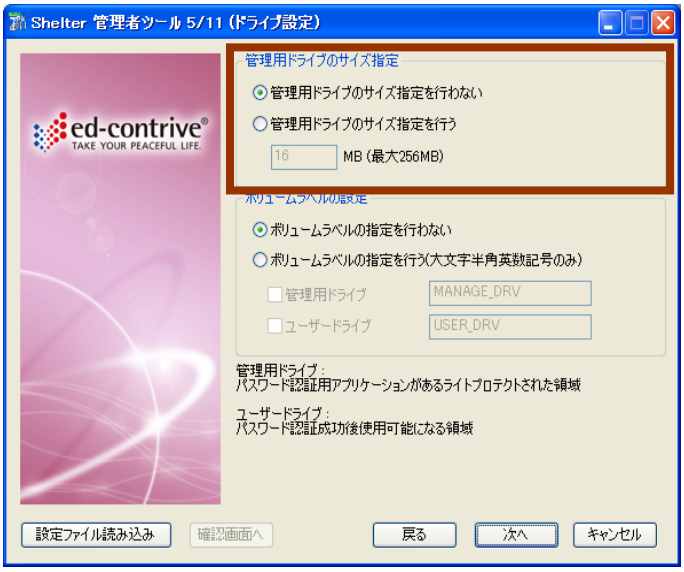
マスターパスワードの設定

マスターパスワードを設定すると、パスワードを忘れた際にも、マスターパスワードを使用してユーザードライブを開くことが可能です。同じ初期化ツールで設定した SD-Shelter 全てに対して、マスターパスワードが有効になりますので、マスターパスワードの設定、取り扱いについてはご注意ください。

マスターパスワードの設定が完了したら、［次へ］をクリックします。

ドライブサイズの設定

管理用ドライブのサイズを 16MB～256MB の範囲で設定することが可能です。管理用ドライブに割り当てた残りがユーザードライブに割り当てられます。
割り当てる容量は 2 の倍数で設定してください。

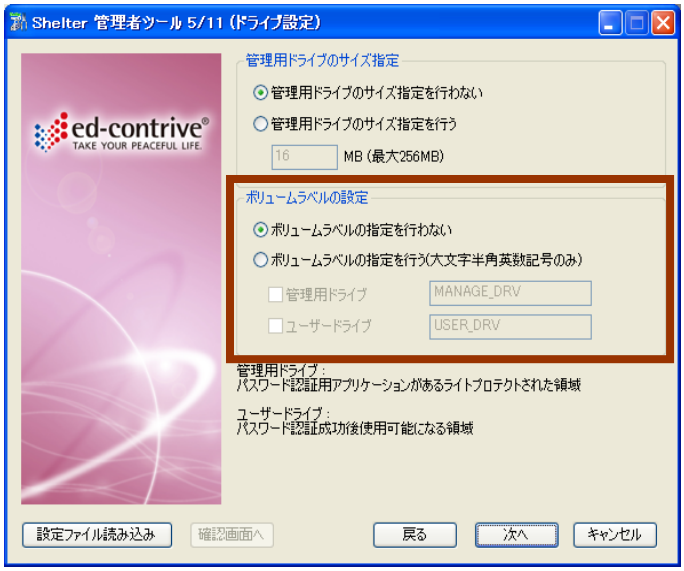


ボリュームラベルの設定

ボリュームラベルをデフォルトから変更することが可能です。
デフォルト設定は以下の通りです。

管理用ドライブ：MANAGE_DRV
ユーザードライブ：USER_DRV

尚、ボリュームラベルは大文字半角英数記号のみ使用できます。



ドライブ設定が完了したら、[次へ] をクリックします。

追加ファイルの設定

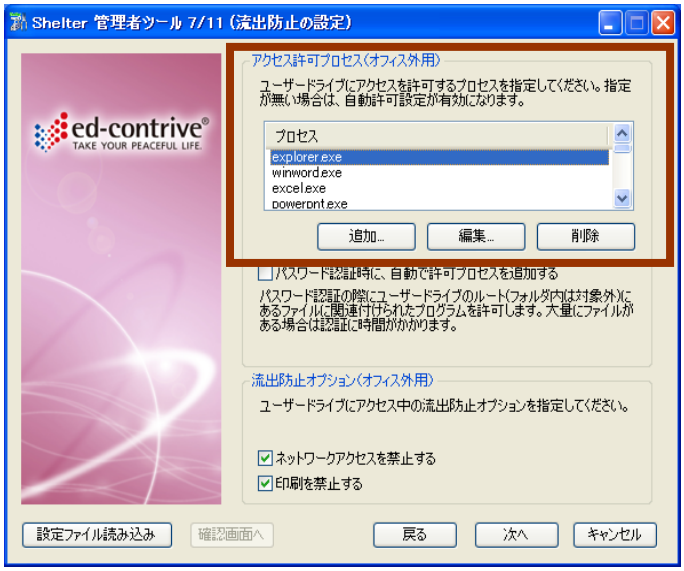
予め、任意のファイルを SD-Shelter に追加しておくことが可能です。ファイルの追加先ドライブをチェック後、ファイルをドラッグ＆ドロップしてください。

尚、管理用ドライブのファイルはユーザーでの削除はできません。
但し、SD-Shelter 外へのコピーや保存は可能なドライブですので、ご注意ください。

追加ファイルの容量に伴い、初期化ツールの容量も増加します。

追加ファイルの設定が完了したら、[次へ] をクリックします。

アクセス許可プロセス（オフィス外用）の設定－①



オフィス外で SD-Shelter **を使用した場合に適用される設定です。ユーザードライブにアクセスを、行うことができるプロセス*1 を指定します。プロセスを指定することで、アクセスを拒否したいソフト等からの進入を遮断することが可能になります。また、ユーザードライブ内のファイルは、アクセスを許可されたプロセスのファイルだけが、起動することができます。**

指定が無い場合は、［パスワード認証時に、自動で許可プロセスを追加する］（P.14 参照）が有効になります。デフォルト設定は以下の通りです。

explorer.exe：**エクスプローラー** /winword.exe：**ワード** /excel.exe：**エクセル**
powerpnt.exe：**パワーポイント** /msaccess.exe：**アクセス** /notepad.exe：**メモ帳**
wordpad.exe：**ワードパッド** /mspaint.exe：**ペイント** /acrord32.exe：**リーダー**
taro15.exe ～ taro18.exe：**一太郎 2005 ～ 2008**
hanako15.exe ～ hanako18.exe：**花子 2005 ～ 2008** /sanshiro.exe：**三四郎**

***1** OS **からメモリ領域などの割り当てを受けて処理を実行しているプログラム。**

［追加］ボタン

［追加］ボタンをクリックすると、プロセスの追加画面が表示されます。入力エリアに追加したいプロセス名を直接入力するか［参照］ボタンをクリックして、プロセス名を選択してください。

［編集］ボタン

リストに表示されているプロセスを選択後［編集］ボタンをクリックすると、プロセスの編集画面が表示されます。入力エリアに表示されている選択プロセス名を直接編集するか［参照］ボタンをクリックして、プロセス名を選択してください。

［削除］ボタン

リストに表示されているプロセスを選択後［削除］ボタンをクリックすると、選択プロセスはリストから削除されます。

アクセス許可プロセス（オフィス外用）の設定－②

＜［パスワード認証時に、自動で許可プロセスを追加する］チェックボックス＞

本機能を有効にすれば、パスワード認証の際に、ユーザードライブのルートにあるファイルに、関連付けられたプログラム（プロセス）を自動で許可します。

フォルダ内は、対象外です。

大量にファイルがある場合は認証に時間がかかる可能性があります。

認証の際に、ルートに存在しなかったプログラム（プロセス）のファイルを、認証後にルートへ追加した場合は、次回認証（再認証）時に許可されます。

本機能が有効でも、指定プロセス分はアクセス許可プロセスとして有効です。

デフォルトの指定プロセス以外は、情報漏洩リスクが高くなり、動作しないソフトも発生することがあります。

流出防止オプション（オフィス外用）の設定

オフィス外で SD-Shelter を使用した場合に適用される設定です。
それぞれ禁止設定にすると、ユーザードライブが有効な間は、ネットワークへのアクセス又は印刷が不可能になります。
禁止しない場合は、情報漏洩のリスクが高くなります。

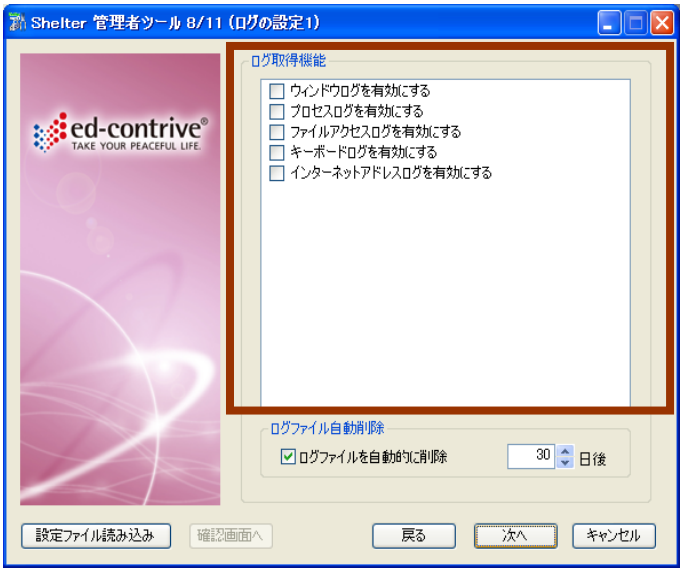
共に、デフォルト設定は禁止するです。

流出防止の設定が完了したら、［次へ］をクリックします。

ログ取得機能の設定

記録したいログの種類をリストより、選択してください。
全て未選択の場合は、ログの取得は行いません。

デフォルト設定は全て未選択です。



ユーザードライブが有効な間は、有効設定のログを取得して、ログファイルに蓄積します。

ログファイルは、SD-Shelter ユーザードライブの Log フォルダ（ログ取得が有効な場合に自動作成）内に、日付単位に複数作成されます。例）080601.log や 080602.log 等

管理者ツールがインストールされているパソコンでのみ、ログファイル内容の閲覧が可能になります。

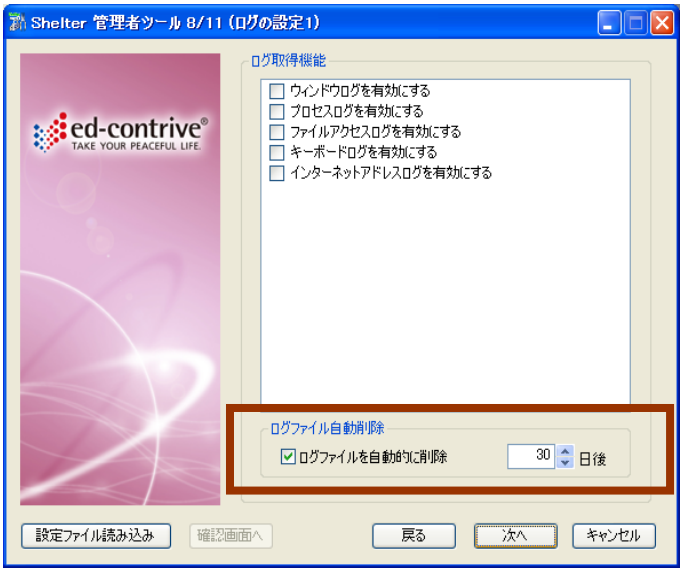
管理者ツールがインストールされているパソコンで、ログを取得させたい場合は、Shelter オフィス内ドライバ又は Shelter オフィス外ドライバのインストールがあわせて必要になります。

ログファイルの表示内容
例）
08/06/01 16:16:33,プロセス,「Excel.exe」が起動しました
08/06/01 16:16:33,ファイルアクセス,「Excel.exe」が「C:¥ed.xls」にアクセスしました
08/06/01 16:16:33,ウィンドウ,「Microsoft Excel - ed.xls」が開きました
08/06/01 16:16:46,キーボード,「S」が押されました
08/06/01 16:17:32,インターネットアドレス,「http://www.ed-contrive.co.jp/」-「イーディーコントライブ」にアクセスしました

ログファイル自動削除の設定

ログファイルを自動的に削除する場合は選択し、日付単位に複数作成される各ログファイルを作成日より何日後に削除するか設定してください。
ユーザーはログファイルを削除できないため、設定することをおすすめ致します。

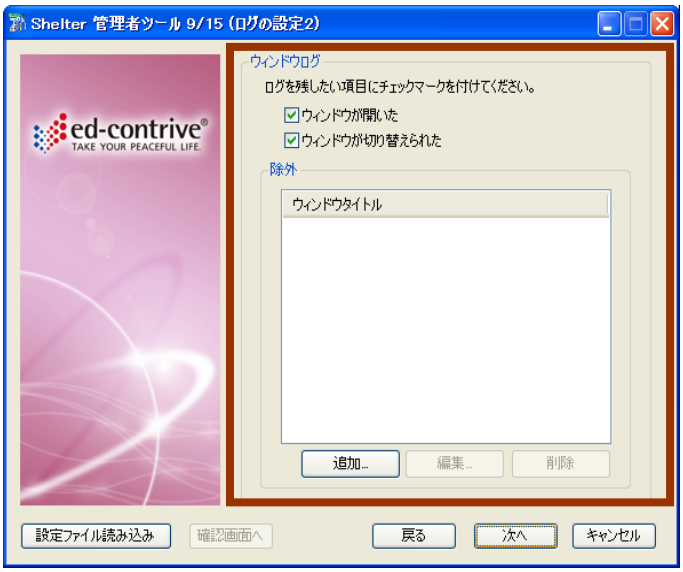
デフォルト設定は 30 日後自動的に削除するです。



ログの設定１が完了したら、［次へ］をクリックします。

ウィンドウログの設定

ログ取得機能の設定で、ウィンドウログを有効にした場合に、設定が可能になります。
ウィンドウログとして残したい項目を選択してください。
ログに残したくないウィンドウタイトルは、除外リストに追加してください。



［ウィンドウが開いた］チェックボックス
開いたウィンドウのウィンドウタイトルを記録します。

［ウィンドウが切り替えられた］チェックボックス
ウィンドウが切り替えられて、アクティブになったウィンドウタイトルを記録します。

除外［追加］ボタン *1
［追加］ボタンをクリックすると、除外ウィンドウタイトルの追加画面が表示されます。
入力エリアに追加したいウィンドウタイトル名を直接入力してください。

除外［編集］ボタン *1
リストに表示されている除外ウィンドウタイトルを選択後［編集］ボタンをクリックすると、除外ウィンドウタイトルの編集画面が表示されます。入力エリアに表示されている選択除外ウィンドウタイトル名を直接編集してください。

除外［削除］ボタン
リストに表示されている除外ウィンドウタイトルを選択後［削除］ボタンをクリックすると、選択除外ウィンドウタイトルはリストから削除されます。

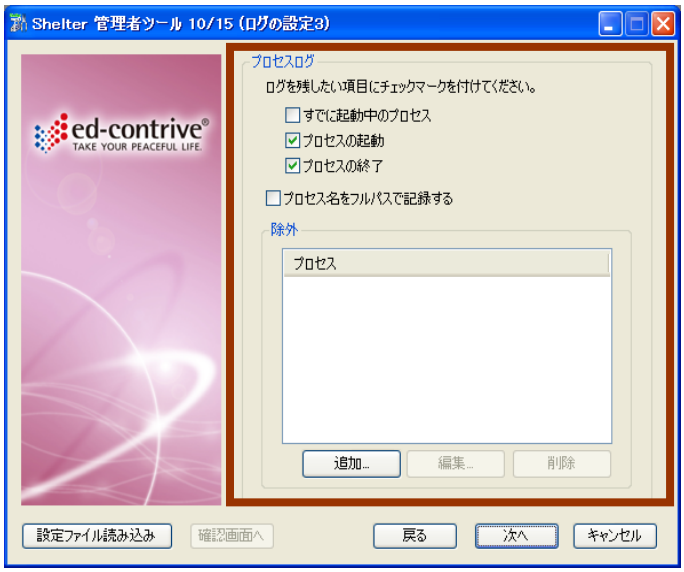
*1 例）Microsoft Excel - ed.xls ：左記に一致するウィンドウタイトルを除外します。

ログの設定２が完了したら、［次へ］をクリックします。

プロセスログの設定

ログ取得機能の設定で、プロセスログを有効にした場合に、設定が可能になります。
プロセスログとして残したい項目を選択してください。
ログに残したくないプロセス*1 は、除外リストに追加してください。

*1 OS からメモリ領域などの割り当てを受けて処理を実行しているプログラム。例）excel.exe



［すでに起動中のプロセス］チェックボックス
ユーザードライブが有効になった時、すでに起動中のプロセスを記録します。

［プロセスの起動］・「プロセスの終了」チェックボックス
それぞれ、プロセスの起動及び終了を記録します。

除外［追加］ボタン
［追加］ボタンをクリックすると、除外プロセスの追加画面が表示されます。入力エリアに追加したいプロセス名を直接入力するか［参照］ボタンをクリックして、プロセス名を選択してください。

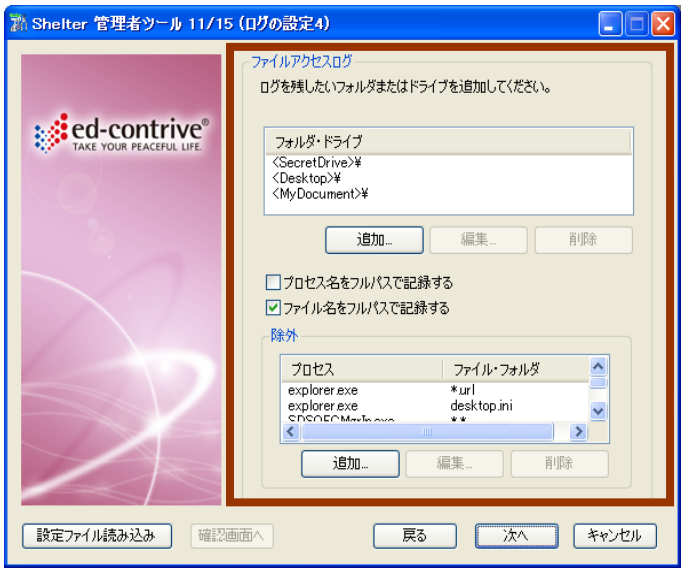
除外［編集］ボタン
リストに表示されている除外プロセスを選択後［編集］ボタンをクリックすると、除外プロセスの編集画面が表示されます。入力エリアに表示されている選択除外プロセス名を直接編集するか［参照］ボタンをクリックして、プロセス名を選択してください。

除外［削除］ボタン
リストに表示されている除外プロセスを選択後［削除］ボタンをクリックすると、選択除外プロセスはリストから削除されます。

ログの設定３が完了したら、［次へ］をクリックします。

ファイルアクセスログの設定－①

ログ取得機能の設定で、ファイルアクセスログを有効にした場合に、設定が可能になります。
ファイルアクセスログとして残したいフォルダ又はドライブを追加してください。
特定のプロセスや OS からアクセスされる、指定のフォルダ又はドライブ以下のファイル又はフォルダへのファイルアクセスログを残したくない場合は除外リストに追加してください。



SecretDrive = **ユーザードライブ**

フォルダ・ドライブ［追加］ボタン（ドライブ全体を指定するとログが大量になります）
［追加］ボタンをクリックすると、フォルダ・ドライブの追加画面が表示されます。**（P.20）**

フォルダ・ドライブ［編集］ボタン（ドライブ全体を指定するとログが大量になります）
リストに表示されているフォルダ・ドライブを選択後［編集］ボタンをクリックすると、フォルダ・ドライブの編集画面が表示されます。**（P.20）**

フォルダ・ドライブ［削除］ボタン（全てを削除した場合は当該ログ全てを取得します）
リストに表示されているフォルダ・ドライブを選択後［削除］ボタンをクリックすると、選択フォルダ・ドライブはリストから削除されます。

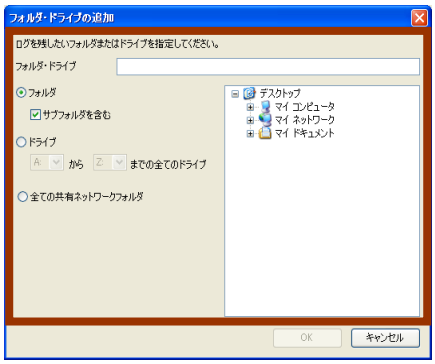
除外［追加］ボタン
［追加］ボタンをクリックすると、除外プロセスの追加画面が表示されます。**（P.20）**

除外［編集］ボタン
リストに表示されている除外プロセス/ファイル・フォルダを選択後［編集］ボタンをクリックすると、除外プロセスの編集画面が表示されます。**（P.20）**

除外［削除］ボタン（デフォルト設定を削除するとログが大量になります）
リストに表示されている除外プロセス/ファイル・フォルダを選択後［削除］ボタンをクリックすると、選択除外プロセス/ファイル・フォルダはリストから削除されます。

ファイルアクセスログの設定－②

＜［フォルダ・ドライブの追加編集］画面＞



［フォルダ・ドライブ］入力エリア *1

左側の［フォルダ］ラジオボタンを選択後、右側のツリー上で選択するか、左側の［ドライブ］又は［全ての共有ネットワークフォルダ］ラジオボタンを選択するとフォルダ又はドライブが入力エリアに表示されます。直接入力も可能で、ファイル名の指定も行えます。

［フォルダ］ラジオボタン

選択することで、右側のツリー上でフォルダ・ドライブの選択が行えます。

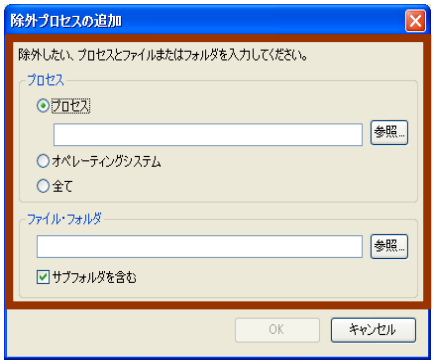
［ドライブ］ラジオボタン

選択することで、ドライブの範囲選択が行えます。

［全ての共有ネットワークフォルダ］ラジオボタン

選択することで、全ての共有ネットワークフォルダを表す文字 \\ が表示されます。

＜［除外プロセスの追加編集］画面＞



［プロセス］ラジオボタン

指定フォルダ・ドライブ以下への、どのプロセスからのアクセスログを除外したいか、直接入力か［参照］ボタンで、そのプロセスを指定します。

［オペレーティングシステム］ラジオボタン

指定フォルダ・ドライブ以下への、OS からのアクセスログを除外します。

［全て］ラジオボタン

指定フォルダ・ドライブ以下への、全プロセスと OS からのアクセスログを除外します。

［ファイル・フォルダ］入力エリア *1

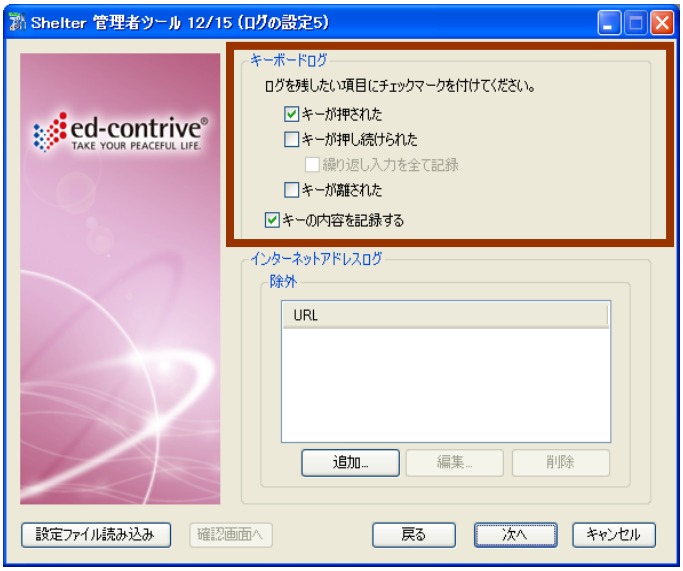
上記、プロセス等からのアクセスログを残したくない指定フォルダ・ドライブ以下のファイル・フォルダを直接入力か［参照］ボタンで指定します。

1 パス無し･絶対/相対パス、ファイル名はワイルドカード指定が可能です。例）C:¥ed¥*.

ログの設定４が完了したら、［次へ］をクリックします。

キーボードログの設定

ログ取得機能の設定で、キーボードログを有効にした場合に、設定が可能になります。
キーボードログとして残したい項目を選択してください。



［キーが押された］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が押されました / 記録しない：キーが押されました

［キーが押し続けられた］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が押し続けられています / 記録しない：キーが押し続けられています

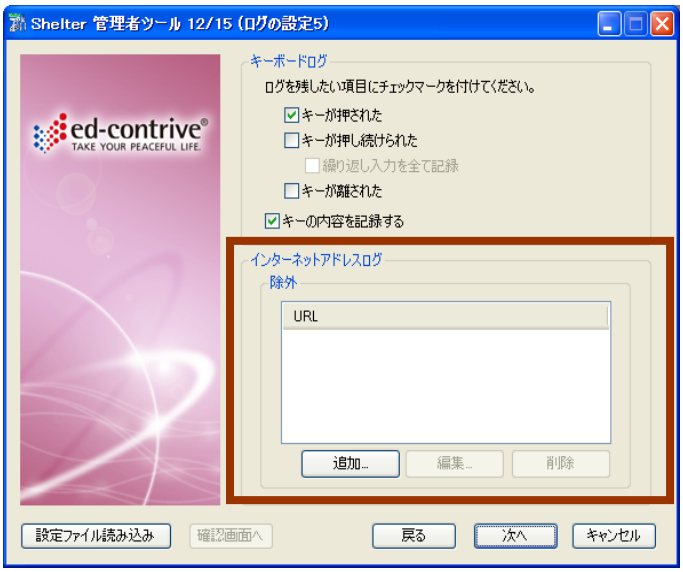
［繰り返し入力を全て記録］チェックボックス
キーが押し続けられている間、繰り返し同一のログを記録します。上記の［キーが押し続けられた］でのログが連続で記録されます。
「繰り返し入力」とは、キーを押したままにした時に、連続的にそのキーが繰り返し入力されたように扱う OS の仕組みのことです。全てを記録することで、何が入力されたかを正確に記録することができますが、記録するログファイルのサイズは大きくなります。

［キーが離された］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が離されました / 記録しない：キーが離されました

［キーの内容を記録する］チェックボックス
選択の場合には、上記例）のように各操作での実際のキーの内容を記録します。
未選択の場合には、上記例）のように各操作での実際のキーの内容は記録しません。

インターネットアドレスログの設定

ログ取得機能の設定で、インターネットアドレスログを有効にした場合に、設定が可能になります。
ブラウザよりアクセスした URL をインターネットアドレスログとして記録します。
対応ブラウザは Internet Explorer（プロトコルは http 又は https）のみです。
ログに残したくない URL は、除外リストに追加してください。



除外［追加］ボタン *1

［追加］ボタンをクリックすると、除外 URL の追加画面が表示されます。入力エリアに追加したい URL を直接入力してください。

除外［編集］ボタン *1

リストに表示されている除外 URL を選択後［編集］ボタンをクリックすると、除外 URL の編集画面が表示されます。入力エリアに表示されている選択除外 URL を直接編集してください。

除外［削除］ボタン

リストに表示されている除外 URL を選択後 [削除] ボタンをクリックすると、選択除外 URL はリストから削除されます。

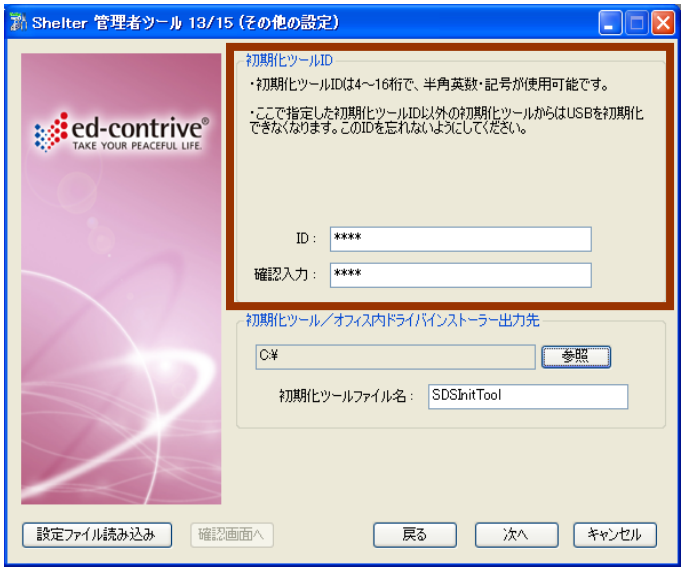
*1 例）

http://www.ed-contrive.co.jp/ ：左記 URL 以下の全ての URL を除外します。

http://www.ed-contrive.co.jp/index.html ：左記に一致する URL を除外します。

ログの設定５が完了したら、［次へ］をクリックします。

初期化ツール ID の設定



初期化ツール ID は、初期化ツール起動時に自動的にチェックされ、ID の異なる初期化ツールでの SD-Shelter の初期化を防止することにより、利用ユーザーによる USB メモリの勝手なポリシー変更を不可能にします。

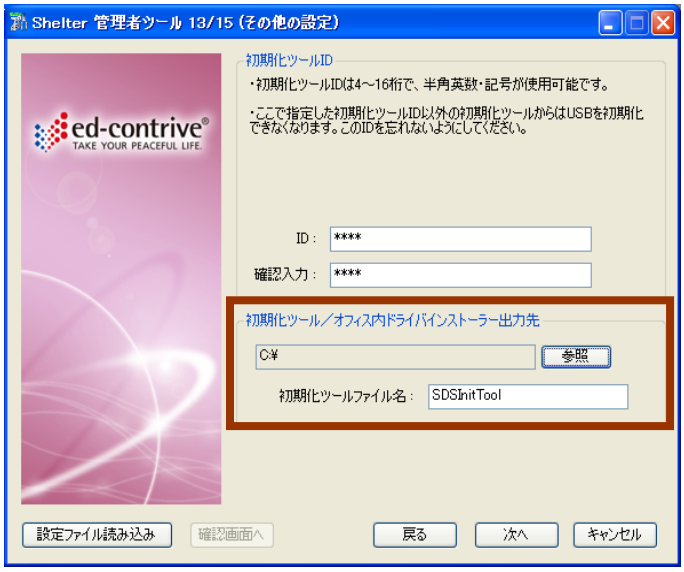
初期化ツール ID はパスワードリマインダ機能、ユーザードライブの遠隔ロック解除機能を利用する場合に必要です。

また、SD-Shelter 起動時には SD-Shelter 側の初期化ツール ID と Shelter オフィス内ドライバ及び Shelter オフィス外ドライバ側の初期化ツール ID が一致した時のみパスワード認証画面を表示させる自動チェック機能にも使用します。

注意	* 新しい初期化ツールを作成して SD-Shelter の書き換えを行う場合には、SD-Shelter 内に既に設定されている初期化ツール ID と同じ ID を入力してください。 * 設定した初期化ツール ID の復元はできません。お客様自身で初期化ツール ID の取扱には十分ご注意ください。

初期化ツール／オフィス内ドライバインストーラーの保存

初期化ツールとオフィス内ドライバインストーラーの出力先、及び初期化ツールのファイル名の設定を行います。



その他の設定が完了したら、［次へ］をクリックします。

設定内容の確認／設定の保存

設定した内容の確認画面が表示されますので、設定内容に問題がなければ［作成］ボタンをクリックし、初期化ツールとオフィス内ドライバインストーラーを作成します。

設定内容を変更するには［戻る］ボタンをクリックします。

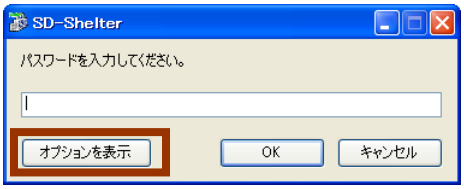
また、［設定保存］ボタンをクリックすることにより、設定した内容を保存しておくことが可能です。

設定した内容は［設定ファイル読み込み］ボタンから読み込むことが可能です。（［設定ファイル読み込み］ボタンは、本画面以前の設定操作時に実行することが可能です）

ユーザードライブ遠隔ロック解除

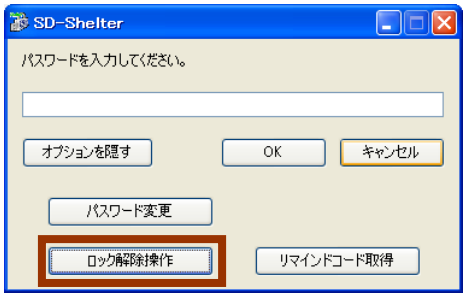
＜SD-Shelter での操作＞

1 パスワード認証画面の［オプションを表示］ボタンをクリックします。



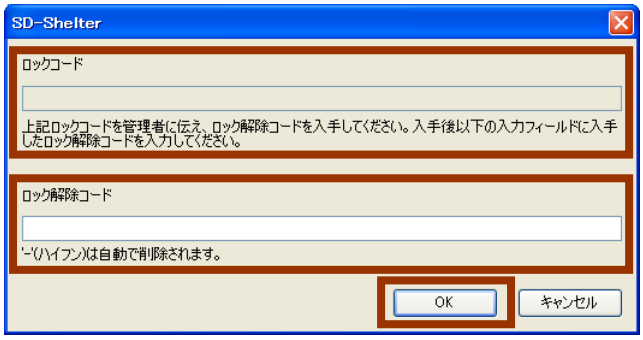
2 ［ロック解除操作］ボタンをクリックします。

* ユーザードライブ遠隔ロック解除機能が有効、且つ、ユーザードライブがロックされた状態の時に［ロック解除操作］ボタンが有効になります。



3 ロックコードが表示されますので、管理者に伝えてください。

4 管理者からロック解除コードを入手後、ロック解除コードを入力し［OK］ボタンをクリックします。



＜Shelter ロック解除ツールでの操作＞

1 ［スタート］→［(すべての) プログラム］→［ED-CONTRIVE］→［Shelter］→［Shelter ロック解除ツール］を選択します。Shelter ロック解除ツールが起動します。

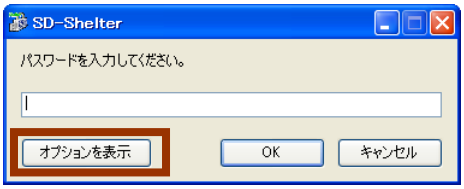
2 初期化ツール ID と SD-Shelter での操作で取得したロックコードを入力し、［生成］ボタンをクリックします。

3 ロック解除コードが表示されますので、ユーザーに伝えてください。

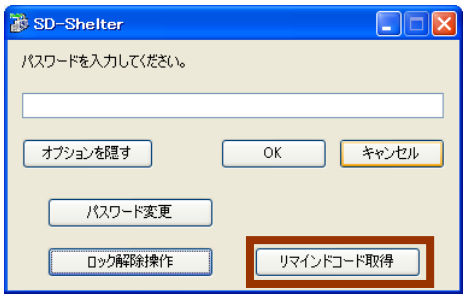
パスワードリマインダ

＜SD-Shelter での操作＞

1 パスワード認証画面の［オプションを表示］ボタンをクリックします。



2 ［リマインドコード取得］ボタンをクリックします。
パスワードリマインダ機能を有効にしていると［リマインドコード取得］ボタンが有効になります。



3 表示されたリマインドコードを控えて、管理者に伝えてください。

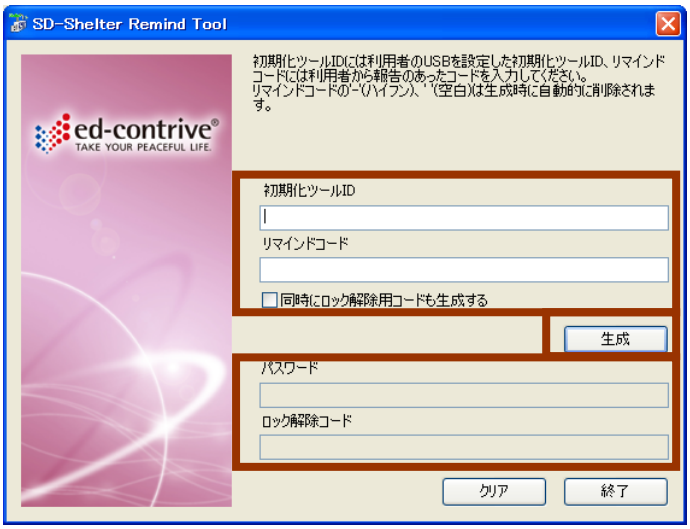
＜Shelter パスワードリマインダでの操作＞

1 ［スタート］→［(すべての) プログラム］→［ED-CONTRIVE］→［Shelter］→［Shelter パスワードリマインダ］を選択します。Shelter パスワードリマインダが起動します。

2 初期化ツール ID と SD-Shelter での操作で取得したリマインドコードを入力します。

3 ［生成］ボタンをクリックすると、パスワードが表示されますので、ユーザーに伝えてください。

［同時にロック解除用コードも生成する］をチェックしていれば、ロック解除コードも同時に生成可能です。



初期化ツールの利用

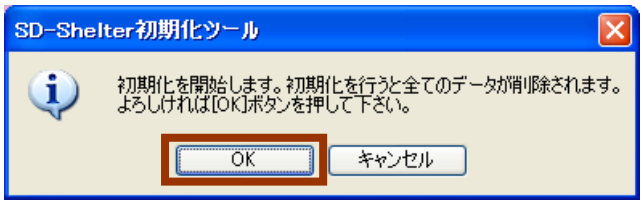
Shelter 管理者ツールで作成した初期化ツールで、SD-Shelter を初期化し、カスタマイズ設定を適用します。同時に「Shelter オフィス外ドライバ」のインストーラーとインストールマニュアル及び Shelter 機能の停止からアンマウントまでを行う「SDSStop」を SD-Shelter 内に作成します。

注意	* 初期化した場合には、USB メモリ内の既存データはログファイルも含め全て失われます。 * 初期化ツールは管理者権限を持つアカウントでのみご使用いただけます。

1 初期化をする SD-Shelter を USB ポートに装着します。

2 初期化ツール（ ）をダブルクリックします。

3 データ削除に関する確認画面が表示されますので、［OK］をクリックします。



4 初期化が開始されます。初期化中、SD-Shelter のドライブに関連のウィンドウが表示されることがありますが、初期化が完了するまでは SD-Shelter を抜かず、操作も行わないようにしてください。

5 完了画面が表示されたら、［OK］をクリックします。

ソフトウェア環境毎の主な機能の比較

下記、ソフトウェア環境下での SD-Shelter の主な機能の比較	ポリシー等の設定	流出防止制御	ﾈｯﾄﾜｰｸｱｸｾｽと印刷
①管理者ツール	可	無	可
②管理者ツール＋オフィス内ドライバ	可	無	可
③管理者ツール＋オフィス外ドライバ	可	有	設定による
④オフィス内ドライバ	不可	無	可
⑤オフィス外ドライバ	不可	有	設定による

下記、ソフトウェア環境下での SD-Shelter の主な機能の比較	アクセス許可プロセス制限	ログの閲覧	ログの記録(取得の場合)
①管理者ツール	無	可	無
②管理者ツール＋オフィス内ドライバ	無	可	有
③管理者ツール＋オフィス外ドライバ	設定による	可	有
④オフィス内ドライバ	無	不可	有
⑤オフィス外ドライバ	設定による	不可	有

* Shelter 管理者ツールと別売の Shelter パスワードリマインダは、同一のパソコンにインストールを行うことはできません。

* Shelter オフィス内ドライバのインストール方法等については、CD-ROM 内のインストールマニュアル（PDF）をご参照ください。

* Shelter オフィス外ドライバのインストール方法等については、SD-Shelter 内のインストールマニュアル（PDF）をご参照ください。

* Shelter オフィス内ドライバと Shelter オフィス外ドライバは、同一のパソコンにインストールを行うことはできません。

* SDSStop.exe の実行以外での SD-Shelter の取り外し（タスクトレイの安全な取り外しや、ツールを使用した取り外し等）は、制御するプログラムの停止等ができないため、行わないようにしてください。必ず、SDSStop.exe を実行して SD-Shelter の取り外しを行ってください。

ソフトウェア使用許諾書

1　本ソフトウェアは、イーディーコントライブ株式会社の著作物です。したがって、本ソフトウェア及び本書の全部または一部を無断で複製、複写、転載、改変することは法律で禁じられています。

2　本ソフトウェア及び本書の内容については､改良のために予告なく変更することがあります。

3　弊社（その許諾者含む）は、お客様、あるいは他の第三者に対して、一切の明示あるいは黙示の保証を行いません。また、本ソフトウェアの機能がお客様の要求に合致していることも、本ソフトウェアに欠陥がないことも一切保証致しません｡本ソフトウェアの使用または使用できないことにより生じる損害、費用、派生的損害、間接的損害、付随的損害、特別損害、または利益の損失につき、いかなる責任も負いかねますので、予めご了承ください。

4　本ソフトウェアの著作権等の知的財産は､いかなる場合においてもお客様に移転されません。

5　本ソフトウェアのソースコードについては、いかなる場合においてもお客様に開示、使用許諾を致しません。また、ソースコードを解析するため本ソフトウェアを解析し、逆アセンブルや逆コンパイル、またはその他のリバースエンジニアリングをすることを禁止します。

6　書面による事前の承諾を得ずに本ソフトウェアをタイムシェアリング、リース、レンタル、販売、移転、サブライセンスすることを禁止します。

7　本製品に関し、日本国内でのみテクニカルサポート及びアフターサービス等を行っております。

8　本ソフトウェアは､「外国為替及び外国貿易法」の規定により戦略物資等輸送既製品に該当する場合があります｡国外に持ち出す際には、日本国政府の輸出許可申請などの手続きが必要になる場合があります。

9　本ソフトウェアは医療機器や人命に直接間接的に関わるシステム、高い安全性が要求される設備や機器に組み込んでの使用は意図されておりません｡これらのシステムや設備等に本ソフトウェアを使用され、本ソフトウェアの動作により人身事故、火災事故、社会的損害などが生じても、当社はいかなる責任も負いかねます。また、高い信頼性が要求される機器や電算機システムなどの用途に使用するときは､ご使用になるシステム等の安全設計や故障に対する適切な処置を万全に行ってください。

10 本ソフトウェアは、一時に一台のパソコンにおいてのみ使用することができます。

11 本ソフトウェアまたはその使用権を第三者に再使用許諾、譲渡、移転等の処分を行うことを禁止します。

12 本ソフトウェアに起因する債務不履行または不法行為に基づく損害賠償は、当社に故意または重大な過失があった場合を除き、本ソフトウェアの購入代金と同額を上限と致します。

13 当社は、お客様が上記のいずれかに違反された場合は、いつでも本ソフトウェアの使用を終了させることができるものとします。